Local Invariants for a Class of Mixed States

Sergio Albeverio[a 1], Shao-Ming Fei[a,b 2], Debashish Goswami[c 3]

[a] Institut für Angewandte Mathematik, Universität Bonn, D-53115
[b] Department of Mathematics, Capital Normal University, Beijing 100037
[c] Statistics and Mathematics Unit, Indian Statistical Institute, Kolkata 700108

Abstract

We investigate the equivalence of quantum states under local unitary transformations. A complete set of invariants under local unitary transformations is presented for a class of mixed states. It is shown that two states in this class are locally equivalent if and only if all these invariants have equal values for them.

PACS numbers: 03.67.-a, 02.20.Hj, 03.65.-w

Quantum entangled states are playing very important roles in quantum information processing and quantum computation [1]. The properties of entanglement for multipartite quantum systems remain invariant under local unitary transformations on the subsystems. Hence the entanglement can be characterized by all the invariants under local unitary transformations. A complete set of invariants gives rise to the classification of the quantum states under local unitary transformations. Two quantum states are locally equivalent if and only if all these invariants have equal values for these states. In [2, 3], a generally non-operational method has been presented to compute all the invariants of local unitary transformations. In [4], the invariants for general two-qubit systems are studied and a complete set of 18 polynomial invariants is presented. In [5] the invariants for three qubits states are also discussed. In [6] a complete set of invariants for generic density matrices with full rank has been presented.

In the present paper we investigate the invariants for arbitrary (finite-) dimensional bipartite quantum systems. We present a complete set of invariants for a class of quantum

[1]SFB 611; BiBoS; IZKS; CERFIM(Locarno); Acc. Arch.; USI(Mendriso)
e-mail: albeverio@uni-bonn.de
[2]e-mail: fei@uni-bonn.de
[3]research partially supported by Av Humboldt Foundation;
e-mail: goswamid@isical.ac.in

mixed states and show that two of these density matrices are locally equivalent if and only if all these invariants have equal values for these density matrices.

1 Invariants for a class of states with arbitrary rank

Let us consider a general mixed state ρ in a bi-partite $n\times n$ system $H\otimes H$ $(n\geq 2)$, with a given orthonormal basis $\{|1>,...,|n>\}$ of H. ρ has the eigen-decomposition

$$\rho=\sum_{l=0}^{N}\mu_l|\xi_l><\xi_l|,$$

where the rank of ρ is $r(\rho)=N+1$ $(N\geq 1)$, μ_l are eigenvalues with the eigenvectors $|\xi_l>=\sum_{ij}\xi_{ij}^{(l)}|ij>$ (and $|\xi_l><\xi_l|$ denotes, as usual, the projector onto $|\xi_l>$), $\xi_{ij}^{(l)}\in\mathbb{C}$. Let A_l denote the matrix with entries $\xi_{ij}^{(l)}$. We call a matrix "multiplicity free" if each of its singular values has multiplicity one. Let $\mathcal{F}$ denote the class of states ρ for which A_0 is multiplicity free. We shall find a complete set of local invariants for the class $\mathcal{F}$, such that any pair of states belong to $\mathcal{F}$ are equivalent under local unitary transformations if and only if they have the same values of these invariants.

Let $(\psi_1,...\psi_n)$, $(\eta_1,...,\eta_n)$ be orthonormal bases such that $A_0=\sum_i\lambda_i|\psi_i><\eta_i|$ is the singular value decomposition of A_0, where $\lambda_1>...>\lambda_n$ denote the singular values arranged in the decreasing order. Let $b_{ij}^{(l)}:=<\psi_i|A_l\eta_j>$ for $l=1,2,...,N$, and for positive integers $k,r\geq 1$, and multi-indices $\underline{i}=(i_1,...i_{k+1})$, (with i_p's all distinct), $\underline{j}=(j_1,...,j_{r+1})$ (with j_q's all distinct), where $i_p,j_q\in\{1,...,n\}$ $\forall p,q$, $\underline{l}=(l_1,...,l_k)$, $\underline{m}=(m_1,...,m_r)$ $(l_t,m_s\in\{1,...,N\})$ with $i_1=j_1$, $i_{k+1}=j_{r+1}$, and such that $(\underline{i},\underline{l})\neq(\underline{j},\underline{m})$, we define

$$I^\rho(\underline{i},\underline{j},\underline{l},\underline{m}):=\frac{b_{i_1i_2}^{(l_1)}...b_{i_ki_{k+1}}^{(l_k)}}{b_{j_1j_2}^{(m_1)}...b_{j_rj_{r+1}}^{(m_r)}}\tag{1}$$

whenever the denominator in the above formula is nonzero. Let Σ^ρ be the set of $(\underline{i},\underline{j},\underline{l},\underline{m})$ such that $I^\rho(\underline{i},\underline{j},\underline{l},\underline{m})$ is well defined.

The following theorem is an immediate consequence of Lemma 6, Lemma 7 and the remark 5.

Theorem 1 *Two quantum states in $\mathcal{F}$ with the same rank and eigenvalues μ_l, $l=0,...,N$, are equivalent under local unitary transformations if and only if they have the same values of the following invariants:*

$$\begin{array}{ll}1) & \text{Matrices } (B_l)_{ij}=|<\psi_i,A_l\eta_j>|,\quad i,j=1,...,n,\ l=1,...,N,\\ 2) & \text{Vector } C=(<\psi_1,A_0\eta_1>,...,<\psi_n,A_0\eta_n>),\\ 3) & \text{Vectors } D_l=(<\psi_1,A_l\eta_1>,...<\psi_{n-1},A_l\eta_{n-1}>),\quad l=1,...,N,\\ 4) & I^\rho \text{ with the domain } \Sigma^\rho.\end{array}\tag{2}$$

Proof : It is clear that the quantities above are local invariant. Let us prove that these invariants are complete for the class $\mathcal{F}$. Suppose that ρ and ρ' are two states in the class $\mathcal{F}$ such that they have the same values of these invariants. Let $\rho = \sum_{l=0}^{N} \mu_l|\xi_l >< \xi_l|$ and $\rho' = \sum_{l=0}^{N} \mu_l|\xi_l' >< \xi_l'|$ be the eigen-decomposition of the two states, and let $A_l = (a_{ij}^{(l)})$, $A_l' = (a_{ij}'^{(l)})$ be $n \times n$ complex matrices associated with the decomposition of ξ_l and ξ_l' respectively, that is, $\xi_l = \sum_{ij} a_{ij}^{(l)}|ij >$, and $\xi_l' = \sum_{ij} a_{ij}'^{(l)}|ij >$. By assumption, A_0 and A_0' are multiplicity-free, with the singular-value decomposition

$$A_0 = \sum_i \lambda_i|\psi_i >< \eta_i|, \qquad A_0' = \sum_i \lambda_i'|\psi_i' >< \eta_i'|,$$

with the singular values arranged in the decreasing order. Since $\lambda_i =< \psi_i, A_0\eta_i >$ and $\lambda_i' =< \psi_i', A_0'\eta_i' >$, it follows that $\lambda_i = \lambda_i'$ for all i. Set $(B_l)_{ij} =< \psi_i, A_l\eta_j >$, $(B_l')_{ij} =< \psi_i', A_l'\eta_j' >)$ for $l = 0, 1, ..., N$. It is easy to see from the equalities of $I^\rho(\underline{i}, \underline{j}, \underline{l}, \underline{m})$ and $I^{\rho'}(\underline{i}, \underline{j}, \underline{l}, \underline{m})$ that the condition (III) of Lemma 6 holds. The conditions (I) and (II) of Lemma 6 also follows from the equalities of the invariants labeled by 3) and 1) in (2) respectively. Thus, by Lemma 7 of Appendix, we conclude that there exist unitary matrices U and V such that $UA_lV^* = A_l'$ for $l = 0, 1, ..., N$. Clearly, we have, $\xi_i' = \sum_{ij} {a^{(l)}}'_{ij}|ij >= \sum_{ij}\sum_{kl} u_{ik}a_{kl}\overline{v}_{jl}|ij >= \sum_{kl} a_{kl}(\sum_i u_{ik}|i >) \otimes (\sum_j \overline{v}_{jl}|j >) = (U \otimes \bar{V})\xi_l$, where $U = (u_{ij})$, $V = (v_{ij})$, $\bar{V} = (\bar{v}_{ij})$. Thus, $\rho' = (U \otimes \bar{V})\rho(U \otimes \bar{V})^*$. $\square$

As an example we calculate all the invariants for the Werner state [7], $\rho_w = (1-p)I_{4\times4}/4 + p|\Psi_- >< \Psi_-|$, where $0 \le p \le 1$, $I_{4\times4}$ is the 4×4 identity matrix and $|\Psi_- >= \frac{1}{\sqrt{2}}(|01 > -|10 >)$.

Here, $N = 3$, $\mu_1 = \mu_2 = \mu_3 = \frac{1-p}{4}$, $\mu_4 = \frac{3p+1}{4}$. We have,

$$\xi_0 = |00 >, \quad \xi_1 = |11 >, \quad \xi_2 = \frac{1}{\sqrt{2}}(|01 > +|10 >), \quad \xi_3 = \frac{1}{\sqrt{2}}(|01 > -|10 >).$$

Hence $A_0 = \begin{pmatrix} 1 & 0 \\ 0 & 0 \end{pmatrix}$, $A_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $A_2 = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 \end{pmatrix}$, $A_3 = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} \\ -\frac{1}{\sqrt{2}} & 0 \end{pmatrix}$. The orthonormal bases $\{\psi_1, \psi_2\}$ and $\{\eta_1, \eta_2\}$ can be chosen to be the canonical basis $\{|0 >, |1 >\}$. Thus, $(B_l)_{ij} = | < \psi_i, A_l\eta_j > | = |(A_l)_{ij}|$ in this case. The invariants are:

1)$B_1 = \begin{pmatrix} 0 & 0 \\ 0 & 1 \end{pmatrix}$, $B_2 = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 \end{pmatrix}$, $B_3 = \begin{pmatrix} 0 & \frac{1}{\sqrt{2}} \\ \frac{1}{\sqrt{2}} & 0 \end{pmatrix}$;

2) $C = (1, 0)$;

3) $D_l = 0$, $l = 1, 2, 3$;

4) $\Sigma^\rho = \{((i_1, i_2), (j_1, j_2), (l_1), (m_1));\ \ l_1, m_1 \in \{2, 3\}, i_p, j_q \in \{1, 2\},\ i_1 \ne i_2, j_1 \ne j_2,\ (i_1, i_2, l_1) \ne (j_1, j_2, m_1)\}$, which can be explicitly written as:

$\{((1, 2), (1, 2), (2), (3)); ((1, 2), (1, 2), (3), (2)); ((1, 2), (2, 1), (2), (2)); ((1, 2), (2, 1), (2), (3));$
$((1, 2), (2, 1), (3), (2)); ((1, 2), (2, 1), (3), (3)); ((2, 1), (1, 2), (2), (2)); ((2, 1), (1, 2), (2), (3));$
$((2, 1), (1, 2), (3), (2)); ((2, 1), (1, 2), (3), (3)); ((2, 1), (2, 1), (2), (3)); ((2, 1), (2, 1), (3), (2))\}$. The values of I^ρ on the above elements (in the same order) are $1, 1, 1, -1, 1, -1, 1, 1, -1, -1, -1, -1$.

Remark 2 *The class of states $\mathcal{F}$ for which our result works is indeed a large one. In fact, $\mathcal{F}\bigcap\mathcal{F}_k$ is dense (in norm) in $\mathcal{F}_k$, where $\mathcal{F}_k$ denotes the set of $n\times n$ bipartite states of rank $k+1$, $k\geq 0$. Consider any state $\rho\in\mathcal{F}_k$, with the eigen-decomposition $\rho=\sum_{l=0}^{k}\mu_l|\xi_l><\xi_l|$, with $\xi_l=\sum_{ij}\xi_{ij}^l|ij>$, and suppose that $A_0:=(\xi_{ij}^0)_{ij=1}^n$ is not necessarily multiplicity-free. We claim that for any $\epsilon>0$, we can choose an $n\times n$ multiplicity-free matrix $A_0'=(a_{ij}')$ such that $|a_{ij}-a_{ij}'|\leq n\epsilon\;\forall\; i,j$. Indeed, if $A_0=\sum_i\lambda_i|\psi_i><\eta_i|$ is the singular value decomposition of A_0, where λ_i's may not be all distinct, we can choose λ_i''s which are distinct among themselves, with $|\lambda_i-\lambda_i'|\leq\epsilon$ for all i. A_0' can be taken to be the matrix $\sum_i\lambda_i'|\psi_i><\eta_i|$. Now, A_0' is multiplicity-free, and if we choose $\rho'=\mu_0|\xi_0'><\xi_0'|+\sum_{l=1}^{k}\mu_l|\xi_l><\xi_l|$, where $\xi_0'=\sum_{ij}a_{ij}'|ij>$, it is easy to see that $\rho'\in\mathcal{F}_k\bigcap\mathcal{F}$ and $\|\rho-\rho'\|\leq 2n^3\epsilon$.*

2 The invariants for another class of rank two states

We now consider another class of states which are rank two states on $\mathbb{C}^n\times\mathbb{C}^n$ such that the matrices A_0, A_1 are of the following form :

$$A_0=pP+(1-p)(1-P),\qquad A_1=qQ+(1-q)(1-Q), \tag{3}$$

where $0<p$, $q<1$ and P, Q are projection operators. We denote this class of states by $\mathcal{G}$.

Theorem 3 *The following is a complete set of local invariants for the states in class $\mathcal{G}$:*

$$\begin{array}{l} Tr(\rho^2),\quad Tr(A_0^2),\quad Tr(A_1^2);\\ Tr[((2P-1)(2Q-1))^k],\quad Tr[((2P-1)E_\pm)^k],\quad k=1,...,n, \end{array} \tag{4}$$

where $E_\pm$ denotes the projection onto the eigenspace of $(2P-1)(2Q-1)$ corresponding to the eigenvalue ±1.

Proof : Clearly, the above quantities are local invariants. We show that they are complete. Let ρ' be another state in $\mathcal{G}$., with p', q', P' and Q' instead of p, q, P and Q respectively. Since ρ has two eigenvalues and $Tr(\rho)=1$, the eigenvalues are determined by $Tr(\rho^2)$. Similarly, $Tr(A_0^2)$ and $Tr(A_1^2)$ completely determine p and q. Thus, $p=p'$ and $q=q'$. Furthermore, by Lemma 8, the equality of the traces $Tr[((2P-1)(2Q-1))^k]$, $Tr[((2P-1)E_\pm)^k]$, $k=1,...,n_i$, with their primed counterparts implies that we can find unitary matrix U such that $UPU^*=P'$, $UQU^*=Q'$. This proves that ρ and ρ' are locally equivalent. □

This Theorem applies to a class of d-computable states [9], with a slight modification as follows. Consider a fixed local unitary operator $W=T_1\otimes T_2$, and let $\mathcal{G}_W$ denote the set of states ρ such that $W\rho W^*\in\mathcal{G}$. Clearly, any two states ρ and ρ' in $\mathcal{G}_W$ are locally equivalent if and only if $W\rho W^*$ and $W\rho' W^*$ in $\mathcal{G}$ are locally equivalent too, which can be determined by computing the invariants (4).

For example, we consider a pure state on $\mathbb{C}^4 \times \mathbb{C}^4$, $|\psi\rangle = \sum_{i,j=1}^4 a_{ij}|ij>$, $a_{ij} \in \mathbb{C}$, $\sum_{i,j=1}^4 a_{ij}a_{ij}^* = 1$. Suppose that the matrix $A = (a_{ij})$ has the form

$$A = \begin{pmatrix} 0 & 0 & a_1 & b_1 \\ 0 & 0 & \bar{b}_1 & d_1 \\ a_1 & b_1 & 0 & 0 \\ \bar{b}_1 & d_1 & 0 & 0 \end{pmatrix}, \tag{5}$$

$a_1, b_1, d_1 \in \mathbb{C}$, satisfying $a_1, d_1 \geq 0$, $a_1 d_1 \geq |b_1|^2$. In this case, $|\psi\rangle$ is a d-computable state and its entanglement of formation is a monotonically increasing function of the generalized concurrence $d = 4(a_1 d_1 - |b_1|^2)$. The entanglement of formation for any mixed states with decompositions on d-computable states can be calculated analytically. Let $|\psi' >= \sum_{i,j=1}^4 a'_{ij}|ij>$ be another pure state with $A' = (a'_{ij})$ of the form (5) and $<\psi'|\psi>= 0$. Then

$$\rho = \mu|\psi><\psi| + (1-\mu)|\psi'><\psi'| \tag{6}$$

is an entangled rank two density matrix. Set $T = \begin{pmatrix} 0 & I_2 \\ I_2 & 0 \end{pmatrix}$ and $W = T \otimes I_4$. As the matrices A, A' are of the form TB, where B is a nonnegative matrix with at most two different eigenvalues with degeneracy two, $\rho \in \mathcal{G}_W$, and the invariants (4) determine the equivalence of two mixed states of the form (6) under local unitary transformations.

3 Remarks and conclusions

We have investigated the equivalence of quantum bipartite states under local unitary transformations. For the states ρ for which A_0 is multiplicity free, as well as for the states ρ which are of rank two on $\mathbb{C}^n \times \mathbb{C}^n$ such that each of the matrices A_0 and A_1 is a nonnegative matrix having at most two different eigenvalues, a complete set of invariants under local unitary transformations is presented. Two of these states are locally equivalent if and only if all these invariants have equal values for them.

The results can be generalized to the multipartite case. For instance, we can consider a tripartite state ρ_{ABC} with subsystems, say, A, B and C as bipartite states $\rho_{A|BC}$, $\rho_{AB|C}$ or $\rho_{AC|B}$. If the conditions in our theorems are satisfied for one of the bipartite decompositions, say $\rho_{A|BC}$, we can judge whether two such tripartite states are equivalent or not under local unitary transformations, in this bipartite decomposition. If they are, we consider further $\rho_{BC} = Tr_A(\rho_{A|BC})$, which is again a bipartite state and can be judged by using our theorems, if the related conditions are satisfied. In this way the equivalence for a class of multipartite states can also be studied according to our theorems.

4 APPENDIX

Lemma 4 *Let $B_l = (b_{ij}^{(l)})$, $C_l = (c_{ij}^{(l)})$ be $n \times n$ matrices with complex entries, $l = 1, ..., N$, where n and N are positive integers. Then there exist complex numbers $u_i, i = 1, ..., n$, with $|u_i| = 1$, $\forall i$ and $c_{ij}^{(l)} = \frac{u_i}{u_j} b_{ij}^{(l)}$ for all $i, j = 1, ..., n$, $l = 1, ..., N$ if and only if the following conditions hold :*
(I) $b_{ii}^{(l)} = c_{ii}^{(l)}$ $\forall i, l$,
(II) $|b_{ij}^{(l)}| = |c_{ij}^{(l)}|$ $\forall i, j, l$,
(III) For all choices of $l_1, ..., l_k, m_1, ..., m_r \in \{1, 2, ..., N\}$ $(k, r \geq 1)$, $i_1, ..., i_{k+1}, j_1, ..., j_{r+1} \in \{1, 2, ..., n\}$ with $i_1 = j_1, i_{k+1} = j_{r+1}$,

$$b_{i_1 i_2}^{(l_1)} b_{i_2 i_3}^{(l_2)} ... b_{i_k i_{k+1}}^{(l_k)} c_{j_1 j_2}^{(m_1)} ... c_{j_r j_{r+1}}^{(m_r)} = c_{i_1 i_2}^{(l_1)} c_{i_2 i_3}^{(l_2)} ... c_{i_k i_{k+1}}^{(l_k)} b_{j_1 j_2}^{(m_1)} ... b_{j_r j_{r+1}}^{(m_r)}.$$

Proof : The proof of the necessity of the conditions (I), (II), (III) is trivial. We prove the sufficiency of these conditions. Assume that (I), (II), (III) are satisfied. We define a relation $\sim$ on the set $\{1, 2, ..., n\}$ as follows. Let us set $i \sim i$ for all i, and for i, j different, let us say $i \to j$ if there exist $i_1, ..., i_{k+1}$ $(k \geq 1)$ with $i_1 = i, i_{k+1} = j$ and $l_1, ..., l_k$ such that $b_{i_1 i_2}^{(l_1)}, b_{i_2 i_3}^{(l_2)}, ..., b_{i_k i_{k+1}}^{(l_k)}$ are all nonzero (by (II) this is equivalent to saying that similar quantities with b replaced by c are all nonzero). We set $i \sim j$ (for different i, j) if $i \to j$ and $j \to i$. It is easy to verify that $\sim$ is an equivalence relation. Let $\{1, 2, ..., n\} = E_1 \bigcup ... \bigcup E_p$ $(p \geq 1)$ be the decomposition into equivalence classes. Choose and fix any $i_1^*, ..., i_p^*$ from $E_1, ..., E_p$ respectively. Set $u_i = 1$ for $i \in \{i_1^*, ..., i_p^*\}$. For any other i, say $i \in E_t$ $(1 \leq t \leq p)$, but $i \neq i_t^*$, we define

$$u_i := \frac{c_{i_1 i_2}^{(l_1)} ... c_{i_k i_{k+1}}^{(l_k)}}{b_{i_1 i_2}^{(l_1)} ... b_{i_k i_{k+1}}^{(l_k)}},$$

where $i_1 = i, i_2, ..., i_k, i_{k+1} = i_t^*$, $l_1, ..., l_k$ are chosen such that $b_{i_1 i_2}^{(l_1)}, ..., b_{i_k i_{k+1}}^{(l_k)}$ are nonzero, which exist as $i \sim i_t^*$. u_i is well defined by (III). Indeed, if any other such "path" $i_1' = i, i_2', ..., i_{r+1}' = i_t^*$, $l_1', ..., l_r'$ is used, we have by (III)

$$\frac{c_{i_1 i_2}^{(l_1)} ... c_{i_k i_{k+1}}^{(l_k)}}{b_{i_1 i_2}^{(l_1)} ... b_{i_k i_{k+1}}^{(l_k)}} = \frac{c_{i_1' i_2'}^{(l_1')} ... c_{i_r' i_{r+1}'}^{(l_r')}}{b_{i_1' i_2'}^{(l_1')} ... b_{i_r' i_{r+1}'}^{(l_r')}},$$

which shows that u_i remains the same if the primed sequence is used. Note also that by (II), we have $|u_i| = 1$ for all i.

With this definition of the u_i,'s we claim that

$$c_{ij}^{(l)} = \frac{u_i}{u_j} b_{ij}^{(l)} \tag{7}$$

for all l, i, j. For $i = j$, (7) follows from (I). In case $b_{ij}^{(l)} = 0$, the relation (7) follows from (II). The only nontrivial case to prove arises when $b_{ij}^{(l)}$ (and hence also $c_{ij}^{(l)}$) is nonzero for $i \neq j$.

Thus, i, j can be assumed to belong to the same equivalence class, say E_t. If $j = i_t^*$, we can take $k = 1$, with $i_1 = i$, $i_2 = j$ in the definition of u_i, and the relation (7) follows. Otherwise, i.e. if $j \neq i_t^*$, we choose sequences $i_1 = i,\ i_2, ..., i_{k+1} = i_t^*,\ l_1, ..., l_k$ for the definition of u_i, and $j_1 = j,\ j_2, ..., j_{r+1} = i_t^*,\ m_1, ..., m_r$ for the definition of u_j, so that

$$\frac{u_i}{u_j}\frac{b_{ij}^{(l)}}{c_{ij}^{(l)}} = \frac{b_{ij}^{(l)} b_{jj_2}^{(m_1)} ... b_{j_r i_t^*}^{(m_r)}}{c_{ij}^{(l)} c_{jj_2}^{(m_1)} ... c_{j_r i_t^*}^{(m_r)}} \cdot \frac{c_{ii_2}^{(l_1)} ... c_{i_k i_t^*}^{(l_k)}}{b_{ii_2}^{(l_1)} ... b_{i_k i_t^*}^{(l_k)}} = 1$$

by (III). This completes the proof of the Lemma. □

Remark 5 *In the statement of the above Lemma, it is easy to see that in the condition (III) it is enough to consider distinct $i_1, i_2, ..., i_{k+1}$ and distinct $j_1, ...j_{r+1}$, as $b_{ii}^{(l)} = c_{ii}^{(l)}$ for all i, l.*

Now we state and prove a result which is a slight variation of Lemma 4, which suits our purpose.

Lemma 6 *Let $B_l = (b_{ij}^{(l)})$, $C_l = (c_{ij}^{(l)})$ be as in Lemma 4, with $n \geq 2$. Then there exist complex numbers $u_i, i = 1, ..., n,\ v_n$ with $|u_i| = 1,\ \forall i,\ |v_n| = 1$, such that $c_{ij}^{(l)} = \frac{u_i}{u_j} b_{ij}^{(l)}$, $c_{in}^{(l)} = \frac{u_i}{v_n} b_{in}^{(l)}$, $c_{nj}^{(l)} = \frac{u_n}{u_j} b_{nj}^{(l)}$ for all $i, j = 1, ..., n-1$ and $l = 1, ..., N$ if and only if the following conditions hold :*
(I) $b_{ii}^{(l)} = c_{ii}^{(l)}\ \forall i = 1, ..., n-1;\ l = 1, ..., N$;
(II) $|b_{ij}^{(l)}| = |c_{ij}^{(l)}|\ \forall i, j = 1, ..., n,\ l = 1, ..., N$;
(III) For all choices of $l_1, ..., l_k, m_1, ..., m_r \in \{1, 2, ..., N\}$ $(k, r \geq 1)$, $i_1, ..., i_{k+1}, j_1, ..., j_{r+1} \in \{1, 2, ..., n\}$ with $i_1 = j_1, i_{k+1} = j_{r+1}$, and with the restriction that $(i_1, ..., i_{k+1})$ are all distinct and so are $(j_1, ..., j_{r+1})$, one has

$$b_{i_1 i_2}^{(l_1)} b_{i_2 i_3}^{(l_2)} ... b_{i_k i_{k+1}}^{(l_k)} c_{j_1 j_2}^{(m_1)} ... c_{j_r j_{r+1}}^{(m_r)} = c_{i_1 i_2}^{(l_1)} c_{i_2 i_3}^{(l_2)} ... c_{i_k i_{k+1}}^{(l_k)} b_{j_1 j_2}^{(m_1)} ... b_{j_r j_{r+1}}^{(m_r)}.$$

Let $N, n \geq 1$ be positive integers, and $A_0, A_1, ..., A_N$; $A_0', A_1', ..., A_N'$ be $n \times n$ positive matrices, $n \geq 2$. Let $(\lambda_1, ..., \lambda_n)$ be the singular values of A_0, and $(\lambda_1', ..., \lambda_n')$ be those of A_0'. Assume furthermore that $(\lambda_1, ..., \lambda_n)$ are all distinct, say, $\lambda_1 > ... > \lambda_n$, and similarly $\lambda_1' > ... > \lambda_n'$. Let $(\psi_1, ...\psi_n)$, $(\eta_1, ..., \eta_n)$ be two orthonormal bases for C^n such that the singular value decomposition of A_0 is given by

$$A_0 = \sum_i \lambda_i |\psi_i >< \eta_i|.$$

Similarly, let $(\psi_1', ..., \psi_n')$ and $(\eta_1', ..., \eta_n')$ are the orthonormal bases corresponding to the singular value decomposition of A_0'. Let matrices B_l, C_l, $l = 1, ..., N$ be defined by $(B_l)_{ij} = b_{ij}^{(l)}$, $(C_l)_{ij} = c_{ij}^{(l)}$, where $b_{ij}^{(l)} =< \psi_i, A_l \eta_j >$, $c_{ij}^{(l)} =< \psi_i', A_l' \eta_j' >$. We have:

Lemma 7 *There exist two unitary matrices U, V such that $UA_lV^* = A'_l$ for all $l = 0, 1, ..., N$ if and only if $\lambda_i = \lambda'_i$ $\forall i$ and the conditions (I), (II) and (III) in the statement of Lemma 6 are satisfied for the choices of $b^{(l)}_{ij}$, $c^{(l)}_{ij}$'s as above.*

Proof : Let V_1, V_2, V'_1, V'_2 be unitary matrices such that $V_1A_0V_2^* = D_0 := diag(\lambda_1, ...\lambda_n)$ and $V'_1A'_0V_2'^* = D'_0 := diag(\lambda'_1, ...\lambda'_n)$. Clearly, $V_1A_lV_2^* = B_l$, $V'_1A'_lV_2'^* = C_l$ for $l = 1, ..., N$.

Proof of the "if" part : Here, $D_0 = D'_0 = D$, say. By Lemma 6, we can find $u_i, i = 1, ..., n$, v_n with $|u_i| = 1$, $|v_n| = 1$, and $c^{(l)}_{ij} = \frac{u_i}{v_j} b^{(l)}_{ij}$ $\forall i, j = 1, ..., n$, $l = 0, ..., N$, with $v_j = u_j$ for $j = 1, ..., n-1$. In other words, $C_l = W_1B_lW_2^*$, $l = 1, ..., N$, where W_l is the unitary given by $W_l := diag(u_1, ...u_n)$ and similarly, $W_2 := diag(u_1, ..., u_{n-1}, v_n)$. We take $U := V_1'^*W_1V_1$, $V = V_2'^*W_2V_2$, and it is easy to verify that $UA_lV^* = A'_l$ for $l = 0, 1, ..., N$.

Proof of the "only if " part : Suppose now that there are unitary matrices U, V such that $UA_lV^* = A'_l$ for $l = 0, 1, ..., N$. It follows from the assumption $UA_0V^* = A'_0$ that $D_0 = D'_0 = D$, say. We have $UA_0V^* = UV_1^*DV_2V^* = V_1'^*DV'_2 = A'_0$, from which it follows that $W_1D = DW_2$, where $W_1 = V'_1UV_1^*$, $W_2 = V'_2VV_2^*$. Thus, $W_1DD^*W_1^* = DW_2^*W_2D^* = DD^*$. Since D is diagonal with all entries distinct and nonnegative, $DD^* = D^2 = diag(\lambda_1^2, ..., \lambda_n^2)$. It follows that W_1 must also be diagonal, i.e. $W_1 = diag(u_1, ..., u_n)$ for some $u_1, ..., u_n$ with $|u_i| = 1$. Similarly, W_2 is diagonal, say $diag(v_1, ..., v_n)$. Furthermore, we have $W_1D = DW_2$, which implies that $\lambda_iu_i = \lambda_iv_i$ for all i, and as $\lambda_1, ..., \lambda_{n-1}$ are strictly positive numbers (only λ_n can possibly be 0), we conclude that $u_i = v_i$ for $i = 1, ..., n-1$. Obviously, $C_l = W_1B_lW_2^*$, from which the conditions (I), (II) and (III) of Lemma 6 follow. □

Lemma 8 *Let (P, Q) and (P', Q') be two pairs of projections in n-dimensional ($n \geq 1$) Hilbert space. There exits a unitary matrix U such that $P' = UPU^*$ and $Q' = UQU^*$ if and only if the following conditions are satisfied:*

$$\begin{array}{ll} (I) & Tr[((2P-1)(2Q-1))^m] = Tr[((2P'-1)(2Q'-1))^m],\ m = 1, ..., n; \\ (II) & Tr[((2P-1)E_\pm)^m] = Tr[((2P'-1)E'_\pm)^m],\ m = 1, ..., n, \end{array} \quad (8)$$

where E_+ and E_- denote the projection onto the eigenspace of the eigenvalue 1 and -1 of the unitary matrix $(2P-1)(2Q-1)$ respectively. $E'_\pm$ are defined similarly, replacing P and Q by P' and Q'.

Proof : The result can be proved by applying the characterization of a pair of projections obtained by Halmos [10] (see also [11] and the references therein for related discussion). We, however, present a direct proof in our finite-dimensional situation.

The "only if" part is trivial. So we suppose that the conditions (I) and (II) hold. Let $S = 2P - 1$, $V = (2P - 1)(2Q - 1)$, and $S' = 2P' - 1$, $V' = (2P' - 1)(2Q' - 1)$. S and S' are selfadjoint unitary matrices, V and V' are unitary ones. We also have $SVS = V^*$,

$S'V'S' = V'^*$. Note that by (I), the eigenvalues of V and V' are the same, and have the same multiplicities. Let Δ be the set of these eigenvalues, and Δ_+ (resp. Δ_-) be the set of eigenvalues with positive (resp. negative) imaginary parts. Furthermore, if we denote by H_λ (resp. H'_λ) the eigenspace of V (resp. of V') corresponding to the eigenvalue λ ($dim(H_\lambda) = dim(H'_\lambda)$, as is already noted), then it is easy to verify that $SH_\lambda = H_{\lambda^{-1}}$, and a similar fact is true for S' and H'_λ. We want to define a unitary U from $\mathbb{C}^n = \oplus_\lambda H_\lambda$ to $\mathbb{C}^n = \oplus_\lambda H'_\lambda$ such that $U = \oplus_\lambda U_\lambda$, where $U_\lambda : H_\lambda \longrightarrow H'_\lambda$ for all λ and $USU^* = S'$. For $\lambda \in \Delta_+$, choose any unitary U_λ from H_λ onto H'_λ (this is possible as H_λ and H'_λ have the same dimension), and then for $\lambda \in \Delta_-$, i.e. $\lambda^{-1} \in \Delta_+$, choose $U_\lambda = S'|_{H'_{\lambda^{-1}}} = U_{\lambda^{-1}} S|_{H_\lambda}$. Finally, we need to define $U_{\pm 1}$, for which we shall make use of (II). By (II), $S|_{H_{+1}} = SE_+$ is unitarily equivalent to $S'E'_+$, so there exists a unitary U_{+1} satisfying $U_{+1} S|_{H_{+1}} U_{+1}^* = S'E'_+$. Similarly, U_{-1} can be defined. By construction, it is clear that $USU^* = S'$ and $UVU' = V'$, which is equivalent to having $UPU^* = P'$ and $UQU^* = Q'$. □

References

[1] M. Nielsen and I.L. Chuang, *Quantum Computation and Quantum Information*, Cambridge University Press, 2000.

[2] E.M. Rains, *IEEE Transactions on Information Theory* **46** 54-59(2000).

[3] M. Grassl, M. Rötteler and T. Beth, *Phys. Rev. A* **58**, 1833 (1998).

[4] Y. Makhlin, *Quant. Info. Proc.* **1**, 243-252 (2002).

[5] N. Linden, S. Popescu and A. Sudbery, *Phys. Rev. Lett.* **83**, 243 (1999).

[6] S. Albeverio, S.M Fei, P. Parashar and W.L. Yang, *Phys. Rev. A* **68** (Rapid Comm.) (2003) 010303.

[7] F.F. Werner, *Phys. Rev. A* **40** (1989) 4277.

[8] M. Horodecki and P. Horodecki, *Phys. Lett. A* **59** (1999) 4206.

[9] S.M. Fei and X.Q. Li-Jost, *Rep. Math. Phys.* **53**(2004)195-210.

[10] P. R. Halmos, *Trans. Amer. Math. Soc.* **144**(1969)381-389.

[11] P. S. Chakraborty, math.OA/0306064 (2003).